435
Application No. 09/453,736

REMARKS

The Examiner rejects claims 1-36 under 35 U.S.C.§102(b) as being anticipated by U.S. Patent 5,671,279 to Elgamal and claims 12 and 25 under 35 U.S.C.§103(a) as being unpatentable over Elgamal as applied to claims 10 and 15 above and further in view of U.S. Patent 5,729,594 to Klingman.

Applicant respectfully traverses the Examiner's rejections. Elgamal and Klingman fail to teach or suggest, individually and collectively, at least the following italicized features of the pending independent claims:

> 1. A method of communicating data between a first computing device and a second computing device, the method comprising the steps of:
> *communicating a first datum of a message from the first computing device to the second computing device with encryption of the first datum; and*
> *communicating a second datum of the message from the first computing device to the second computing device without encryption of the second datum.*
>
> 15. A data communication system comprising:
> a first computing device that communicates information to a second computing device responsive to a request from the second computing device to the first computing device, *the information including a procedure that causes the second computing device to select a first datum of a message for communication of the first datum from the second computing device to the first computing device with encryption and select a second datum of the message for communication of the second datum from the second computing device to the first computing device without encryption*; and
> *the first computing device receiving the first datum with encryption and the second datum without encryption and decrypting the first datum.*
>
> 36. A method of communication data between a first computing device and a second computing device, the method comprising:
> (b) receiving a message from the user, wherein the message comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the display, wherein the first datum is confidential to the user and the second datum is non-confidential to the user;

(c) *identifying that the first datum is confidential and the second datum is non-confidential;*

(d) *the first computing device communicating, to the second computing device, the first datum with encryption; and*

(e) *the first computing device communicating, to the second computing device, the second datum without encryption, wherein steps (d) and (e) occur at least substantially simultaneously.*

The present invention is directed to an encryption module that encrypts only part of a message sent by one node to another node. By way of example, in one configuration of the present invention a graphical display is presented to a user requesting the user to input information into a number of input fields. Some of the fields require the entry of confidential information while others do not. The fields are identified accordingly. When user requests transmission of the displayed information to another node, the module encrypts only the confidential fields and not the non-confidential fields. The use of encryption on only part of the transmission can represent substantial savings in computational resources both at the transmitting and receiving nodes.

Elgamal

Elgamal, the primary reference, is directed to a courier electronic payment system that provides customers, merchants, and banks with a secure mechanism for using a public network as a platform for credit card payment services. The system governs the relationship between a customer, merchant, and acquirer gateway to perform credit card purchases over such networks as the Internet. The system uses a secure connection to simplify the problem of Internet-based financial transactions in accordance with an electronic payment protocol that secures credit card payments and certifies infrastructure that is required to enable all of the parties to participate in the electronic

commerce, as well as to provide the necessary formats and interfaces between the different modules and systems.

The Examiner states that Elgamal teaches sending both encrypted (PI value) and unencrypted (purchase order and payment instruction messages) information from a merchant to a customer. This conclusion conflicts with the clear teachings of Elgamal. At col. 4, lines 33-37, Elgamal states that:

> All channel communications between any two nodes in the system should be encrypted. This guards against any network snooping and does not give any information to possible attackers.

At col. 4, lines 52-57, Elgamal further states that:

> Integrity is maintained at all times using a keyed message digest computation. This should be part of the channel security mechanism. An extra layer of integrity is added to the message level using a hash of each message to avoid early termination type attacks, and to make sure that the messages arrive at the recipient unaltered.

Regarding the specific text identified by the Examiner, Elgamal specifically states that the "PI value should be encrypted so that the Merchant's server, e.g. on the Internet, does not have any clear credit card numbers that can be accessed remotely" (col. 9, lines 30-33) and "[t]he PI is preferably sent encrypted to the Acquirer using the Acquirer's public key" (col. 10, lines 20-21). As admitted by the Examiner, Elgamal does not *specifically* state that the purchase order and payment instruction messages are not encrypted.

Even if the Examiner's reading of Elgamal is correct, Elgamal refers to different messages sent at *differing* times. It does not refer to the encryption of only parts of the same message. In the present invention, the encrypted and unencrypted input fields are requested to be transmitted by the user simultaneously or substantially simultaneously. Within the packeted stream derived by the

present invention from the message, some packet payloads are encrypted while others are not and/or some portions of a packet payload are encrypted while other portions are not.

In the final Office Action, the Examiner counters these arguments by referencing Elgamal, col. 9, lines 30-33, and 61-67, and stating that Elgamal states that PI information is encrypted and *implies* that other fields, such as the order and payment instructions, are not encrypted. This conclusion conflicts with other passages in Elgamal, such as col. 4, lines 33-37 and 52-57 and col. 10, lines 37-40. For example, Elgamal does state that the PI value may be sent "in the clear" (col. 10, lines 21-23) but later states that:

> It may be necessary to send the PI without encryption in case of a merchant that performs the capture process independently. This is reflected in a capability field in the merchant certificate that instructs the acquirer software to send the credit card information back to the merchant. *As discussed above, the data on the channel are encrypted by the secure transport, and the Merchant is the only entity that may receive the clear PI data from the acquirer.*

(Col. 10, lines 37-40 (emphasis supplied).) Even more clearly, Elgamal states:

> The PI is preferably sent encrypted to the Acquirer using the Acquirer's public key. In some cases, due to certain Merchant - Acquirer relationships, the PI may be sent in the clear. It is *always* recommended to encrypt the PI message using the following digital envelope construction.
>
> E(Slip) = PKA{DES key K}, K(Slip)
>
> The final message sent is formatted as follows:
>
> PI = SIGNA(E(Slip))
>
> where the SIGN operation is defined as above.

(Col. 10, lines 20-32 (emphasis supplied.) These passages state that *all* channel communications are encrypted using a keyed message digest computation to avoid early termination-type attacks. Although Elgamal states that the PI information may be sent "in the clear" (without some level of encryption), it also states that all data on a channel is encrypted by the secure transport layer and

therefore "the Merchant is the only entity that may receive the clear PI data from the acquirer." (Col. 10, lines 39-40.) The statement of Elgamal refers to a particular type of encryption being absent, namely encryption using the acquirer's public key, and does not refer to *any and every* type of encryption being absent. The public key is used as discussed at col. 10, lines 25-32, so that the "Merchant's server, e.g., on the Internet, does not have any clear credit card numbers that can be accessed remotely". (Col. 9, lines 29-32.)

Klingman

Klingman is directed to a remote communication system for facilitating secure electronic purchases of goods in on-line, wherein a suitable local user input device in association with a data transmission system, couples the user input into a packet network system for communication to a remote receiver/decoder apparatus to try a potentially desirable product. Upon selection of the desired product by the user, a telecom network link is used to communicate a telephone number associated with the desired product from the user to the remote receiver to allow the user to buy the desired product. The telecom network used to link the user input device to the remote apparatus may also include a 900 number billing system for assessing and collecting fees for use of the system.

Klingman fails to overcome the deficiencies of Elgamal. Klingman, unlike Elgamal and the present invention, sends confidential information over a circuit-switched telecommunications network, such as the PSTN, and non-confidential information over a packet-switched network, such as the Internet. "Consequently, there is no need for any encryption procedures or digital signatures, although encryption may be used if so desired." (Col. 13, lines 45-52.)

Accordingly, the rejected claims are allowable over Klingman.

The dependent claims provide further reasons for allowance.

By way of example, dependent claim 2 requires the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum to include the step of communicating the first datum with encryption and the second datum without encryption in a same packet that comprises the message and further includes the steps of providing a display to a user, the display comprising at least first and second input fields for input from the user and at least a first presentation field associated with the at least first and second input fields; and receiving the message from the user, wherein the message corresponds to the display and wherein first datum refers to the first input field and the second datum to the second input field of the display. *See also* dependent Claim 16.

Dependent claim 3 requires the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum to include the steps of communicating the first datum with encryption in a first packet of the message and communicating the second datum without encryption in a second packet of the message different from the first packet of the message and the further steps of providing a display to a user, the display comprising at least first and second input fields for input from the user and at least a first presentation field associated with the at least first and second input fields and receiving the message from the user, wherein the message corresponds to the display and wherein the first datum refers to the first input field and the second datum to the second input field of the display. *See also* dependent Claim 17.

Dependent claim 4 requires the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum comprise the step of employing a same path between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption. *See also* dependent Claim 18.

Dependent claim 5 requires the step of employing the same path to communicate the first datum with encryption and the second datum without encryption to include the step of employing a TCP/IP passage between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption. *See also* dependent Claim 19.

Dependent claim 6 requires the step of communicating the first datum of the message with encryption of the first datum to include the step of employing a key to encrypt the first datum of the message for communication of the first datum from the first computing device to the second computing device with encryption of the first datum. *See also* dependent Claims 7-9 and 20-22.

Dependent claim 10 requires the step of communicating a procedure from the second computing device to the first computing device, and wherein the step of communicating the first datum of the message from the first computing device to the second computing device with encryption of the first datum comprises the step of employing the procedure to encrypt the first datum of the message for communication of the first datum from the first computing device to the second computing device. *See also* dependent Claims 11-14 and 23-27.

Dependent claims 30-35 are also allowable over the cited art for reasons noted above.

Application No. 09/453,736

Based upon the foregoing, Applicant believes that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: Douglas Swartz

Douglas W. Swartz
Registration No. 37,739
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: May 6, 2004

J:\4366\-41\Ammnd_Resp002.wpd